Release Notes

IBM® Tivoli® Identity Manager

Authentication Manager (ACE) v6.1 Adapter

Version 4.6.5

Tenth Edition (August 9, 2010)

This edition applies to version 4.6 of this Adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

Welcome to the IBM Tivoli Identity Manager ACE Server Adapter.

These Release Notes contain information for the following products that was not available when the IBM Tivoli Identity Manager manuals were printed:

- IBM Tivoli Identity Manager ACE Server Adapter Configuration and Installation Guide

Adapter Features and Purpose

The ACE Server Adapter is designed to create and manage ACE Server accounts and Tokens. This adapter must be installed on the server where ACE is installed. For replicated ACE systems, install one Adapter on the primary ACE server.

The ACE Server Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating accounts and assigning privileges. Operations requested from the Identity Manager server will fail if the Adapter is not given sufficient authority to perform the requested task. IBM recommends that this Adapter run with administrative permissions.

Contents of this Release

Adapter Version

Component	Version
Release Date	August 9, 2010
Adapter Version	4.6.5 (build 4.6.1013)
Comm. Libraries	ADK v4.805
Documentation	ACE Server Adapter Installation and Configuration Guide v4.6.0

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR0615102351	Need all dates managed by the ACE adapter to be handled in the same date format (i.e. Zulu). For more details refer the configuration notes section "Retrieving the token related attributes Value in Zulu or Ace Server local format ".
	Items included 4.6.4 release
	None
	Items included 4.6.3 release
MR0310092030	Support to set new PIN for token. Support to set token in new PIN mode. Support to set PIN to Next Tokencode.
	Items included 4.6.2 release
	None
	Items included 4.6.1 release
	None
	Items included 4.6.0 release
MR1015066031	TIM adapter for RSA ACE 6.1
MR010406401	ITIM Authentication Manager v6.1 adapter
MR0201063345	Support for Ace Server 6.1 (now named RSA Authentication Manager v6.1)
MR0321053434	ACE: Enhancement request for ACE Token Extension Data

Closed Issues

INTERNAL#	APAR#	PMR# / Description
		Items closed in current version
	IZ80200	42110,227,000 Disabled tokens get enabled on modify request.
	IZ73555	87443,227,000 The eracetmpuserenddt attribute is not handled as expected by adapter. For more details refer the configuration notes section “Setting the Start Date and End Date value through ITIM”.
		Items closed in version 4.6.3
	IZ65164	48986,227,000 If any temp user's start or end time is 12:00 AM in GMT, then, adapter fails to modify user account.
	IZ58714	32771,077,649 Unable to modify existing "END DATE" value on an RSA/ACE account from TIM.
		Items closed in version 4.6.3
	IZ61854	20010,227,000 ACE 6.1 adapter fails during recon on SunOs with segmentation violation
		Items closed in version 4.6.2
	IZ55836	81471,227,000 ACE Adapter crash during modify.
36265		N/A Ace adapter crashes on Solaris when Last Name, First Name & PIN value is set as Blank.

INTERNAL#	APAR#	PMR# / Description
		Items closed in 4.6.1 version
N/A	IY96123	50068,L6Q,000 Group name gets truncated by the Ace 5.2 adapter if length is more than 48 characters.
N/A	IY96234	81260,49R,000 Ace adapter crashes when erUID is null. Note on Required AuthMan Attributes: This adapter is configured to require the minimum set of attributes to create an AuthMan account. If you have configured your AuthMan system to require additional attributes, IBM suggests that you use the ITIM Form Designer to make these attributes “required.” IBM further recommends that your Provisioning Policy be configured to supply these required attributes. Example: If the "User-Created Pins required" option is checked on the AuthMan Server and the CREATEPIN attribute is not sent in the ITIM request, the agent will log warning message or fail the request.
		Items closed in 4.6.0 version
		None

Known Issues

Internal#	APAR#	PMR# / Description
		None

Installation and Configuration Notes

See the IBM Tivoli Identity Manager ACE Server Adapter Installation Guide for detailed instructions.

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

Supported Authentication Manager Versions

This adapter supports only Ace Server 6.1. For Ace Server 6.0 and 5.2 please use the ITIM Ace 5.2 adapter.

Account Credentials

During installation, user credentials under which Ace Server 6.1 is installed must be entered. The adapter service will be run under this account. Incorrect configuration may result in adapter service not being started after installation.

Required Environment Variables

For use on AIX the following environment variables must be set before installing this adapter:

1. ACE=`dirname $USR_ACE`
2. DLC=$ACE/rdbms/
3. PROMSGS=$DLC/promsgs
4. PATH=$USR_ACE:$DLC/bin:$ACE/utils:$ACE/utils/oldutil:$PATH
5. PROPATH=$USR_ACE/proapi/adbapi.pl:$USR_ACE/protrig:$USR_ACE/proapi:$USR_ACE
6. LIBPATH=$USR_ACE:$LIBPATH

For use on HP-UX the following environment variables must be set before installing this adapter:

1. ACE=`dirname $USR_ACE`
2. DLC=$ACE/rdbms/
3. PROMSGS=$DLC/promsgs
4. PATH=$USR_ACE:$DLC/bin:$ACE/utils:$ACE/utils/oldutil:$PATH
5. PROPATH=$USR_ACE/proapi/adbapi.pl:$USR_ACE/protrig:$USR_ACE/proapi:$USR_ACE
6. SHLIB_PATH=$USR_ACE:$SHLIB_PATH

For use on Solaris the following environment variables must be set before installing this adapter:

1. ACE=`dirname $USR_ACE`
2. DLC=$ACE/rdbms/
3. PROMSGS=$DLC/promsgs
4. PATH=$USR_ACE:$DLC/bin:$ACE/utils:$ACE/utils/oldutil:$PATH
5. PROPATH=$USR_ACE/proapi/adbapi.pl:$USR_ACE/protrig:$USR_ACE/proapi:$USR_ACE
6. LD_LIBRARY_PATH=$USR_ACE:$LD_LIBRARY_PATH

Configuration Notes

The following corrections to the Installation Guide apply to this release:

Maximum Token Limit:

The ACE/Server limits the number of tokens to three. When assigning a password to a user, the ACE/Server will treat that as a special token, hence, the available numbers of tokens will become two.

Assigning Password:

When applying (assigning) a Password to a user, the Agent must receive the following:

a) The password, passed in the Password attribute.
b) Duration of the password is valid, passed in two attributes:
   - Days attribute (number of days password is valid).
   - Duration attribute (number of hours password is valid).
c) PasswordToken attribute MUST be set to YES.

Un-Assigning Tokens:

When Un-Assigning the Last Tokens from a user, the ACE/Server will delete the user from the database unless one of the following is true:

a) The user belongs to any group
b) The user is enabled on any client.
c) The user is an administrator.
d) The user record has extension fields.

If any of the above is true, the ACE/Server will fail the un-assignment of a token, and the Agent will fail the transaction as well.

In the event where the user is deleted due to un-assigning of the last token, the Agent will re-add the user without any tokens. The Agent will user the existing Login ID, Last Name, First Name, Default Shell and Create PIN mode to re-add the user

Suspend/Restore a User:

Suspending a user implies that all the user's tokens will be disabled.
Restoring a user implies that all the user's tokens will be enabled.

Using the User Extension Data Feature

The user extension data is a key-data pair and must follow these conventions:

Key: Name for the extension data field. The key can be up to 48 characters.
If key contains a colon (":") then it must be escaped with "\".
The key may not contain " , " as this sequence is used by Ace Server while returning
The key-data pair.

Data: Data that you want to store in this field. The value can be up to 80 characters.

Format: The key-data pair must be separated by ":"
Example "key1:value1" where key=key1 and data=value1.

New Features in Version 4.6.3

The following new features have been added to this version of the adapter.

Setting a new PIN for the token:

You can set a new PIN for a token assigned to the user.

Usage:

- The user can specify this value in the 'Set a new PIN' field on the TIM UI. The user can find this field in all the token tabs available on the TIM account form.
- The user can assign this new pin during the ADD or the MODIFY operation.

Setting the token in new PIN mode:

You can set the token in new PIN mode. In this mode, the user initially authenticates with the Passcode generated by the PIN. On successful logon he/she is prompted for change in PIN. This PIN can be system generated or user defined. Then onwards, user has to login with the Passcode generated by the New PIN.

Usage :

- The user can set the token in New PIN mode from the TIM UI by selecting the field 'New Pin mode'. The user can find this field in all the token tabs available on the TIM account form.
- The user can set the token in New PIN mode during the user ADD or the MODIFY operation.

Setting the PIN to Next Tokencode

You can set a PIN for a token to next tokencode. It means that, the PIN can be set with the first n digits of a next tokencode. To achieve this, you have to provide the Current Tokencode with setting the token to Next Tokencode. Then, you will get the number of digits to be used as PIN from the Next Tokencode.

Usage :
The PIN can be set in Next Tokencode only during the user MODIFY operation.
The following are the steps that the user has to follow for setting the PIN in Next Tokencode.

1. Note down current tokencode (for example, "12345678") and next tokencode (for example, "87654321") pair for any time period displayed on RSA SecurID Token Device UI
2. The user has to select the 'Set PIN to Next Tokencode' checkbox on the TIM UI.
3. The user has to type the noted current token code to the field 'Current Tokencode' on the TIM UI. For example, Current Tokencode is "12345678".
4. The new PIN of the token will be the first n digits of the Next Tokencode. For example, Next Tokencode is "87654321".

Then, the user has to send a reconciliation/lookup request from the TIM UI. After performing the reconciliation/lookup request, the user is able to see the value of field 'Number of digits to be used from the Next Tokencode as PIN' on the same token tab. For example, "4".

Then, the user will be able to login to the resource with the new PIN i.e. The new PIN will be the first n (For example, 4 is the number of digits seen in the field 'Number of digits to be used from the Next Tokencode as PIN') digits of the Next Tokencode that has been noted down. For example, "8765" will be the new PIN for the token as these are the first 4 digits of the Next Tokencode "87654321".

The user request for setting the PIN in Next Tokencode will fail if the Next Tokencode starts with 0. This is resource behavior (i.e. the behavior of ACE 5.2).

Notes:

- After the PIN is set in Next Tokencode successfully, the user will find a new user extension data of the type ITIMToken=<Token_number> : <no of digits>. For example, "ITIMToken=101010101 : 4". The user is requested not to change or delete this data, since it is used by the adapter.

- The removal of this user extension data is handled by the adapter appropriately during token unassignement.

- The user may also find a change in the User extension data, when he sets the PIN in Next Tokencode successively.

New Features in Version 4.6.5

The following new features have been added to this version of the adapter.

Retrieving the token related attributes value in Zulu or Ace Server local format:

Below are the date type attributes managed by ace adapter.

Sr.No	Attribute	Label on TIM side	Reconciled only (R) Add/Mod permit(W)
1	eracetmpusrstdt	Start Date	W
2	eracetmpusrenddt	End Date	W
3	erAceToken1ActivationDate	Date Activated(Token#1)	R
4	erAceToken1ShutdownDate	Date Will Shutdown (Token#1)	R
5	erAceToken1EnableDisableDate	Date Enabled/Disabled (Token#1)	R
6	erAceToken1LastLoginDate	Last Login Date (Token#1)	R
7	erAceToken2ActivatedDate	Date Activated (Token#2)	R
8	erAceToken2ShutdownDate	Date Will Shutdown (Token#2)	R
9	erAceToken2EnableDisableDate	Date Enabled/Disabled (Token#2)	R
10	erAceToken2LastLoginDate	Last Login Date (Token#2)	R
11	erAceToken3ActivatedDate	Date Activated (Token#3)	R
12	erAceToken3ShutdownDate	Date Will Shutdown (Token#3)	R
13	erAceToken3EnableDisableDate	Date Enabled/Disabled (Token#3)	R
14	erAceToken3LastLoginDate	Last Login Date (Token#3)	R
15	erAcePasswdActivatedDate	Date Activated (Special Token)	R
16	erAcePasswdShutdownDate	Date Will Shutdown (Special Token)	R
17	erAcePasswdEnableDisableDate	Enabled/Disabled (Special Token)	R
18	erAcePasswdLastLoginDate	Last Login Date (Special Token)	R

The eracetmpusrstdt and eracetmpusrenddt were already managed by adapter in the Zulu format.

To support this enhancement added new registry key “DATE_FORMAT_IN_ZULU” in the adapter.
The expected value will be TRUE or FALSE. Initially default value will be FALSE.

1. DATE_FORMAT_IN_ZULU = TRUE
   - If you set the registry key value to TRUE, then during reconciliation or user Lookup operation the date type attributes value related to the tokens will be return to TIM in Zulu (YYYYMMDDHHMMZ i.e. 201007251021Z) format.
   - **Note**: - In Zulu time format seconds will be ignored.

2. DATE_FORMAT_IN_ZULU = FALSE
   - If you set the registry key value to FALSE, then during reconciliation or user Lookup operation the date type attributes value related to the tokens will be return to TIM in Ace Server local (MM/DD/YYYY HHH:MMM:SSS i.e. 07/24/2010 000:000:000) format.

To modify the value of registry key “DATE_FORMAT_IN_ZULU” use agentcfg tool.

Setting the Start Date and End Date value through ITIM.

Following Scenarios should be consider to avoid loss of minutes from erAceTmpUsrStDt “Start Date” and erAceTmpUsrEndDt “End Date” attributes while setting them from ITIM Side.

All the scenarios listed below are applicable to End Date also.

1. If time zones of ITIM and Ace Server are same

   A. If ITIM and Ace Server time zones are GMT +/– **X: 00**
   For example: - ITIM and Ace Server time zones are GMT - 05:00 then you must set minutes as 0 (refer case 1 from Table 1). If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer case 2 from Table 1).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5	Start Date 04/06/2010 06.00 PM	GMT - 5	04/06/2010 18.00	04/06/2010 06.00 PM
2	GMT - 5	Start Date 04/06/2010 06.30 PM	GMT - 5	04/06/2010 18.00	04/06/2010 06.00 PM

Table 1

   B. If ITIM and Ace Server time zones are GMT +/– **X: 30**
   For example: - ITIM and Ace Server time zones are GMT + 05:30 then you must set minutes as 0 (refer Case 1 from Table 2). If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer Case 2 from Table 2).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT + 5:30	Start Date 04/06/2010 05.00 AM	GMT + 5:30	04/06/2010 05.00	04/06/2010 05.00 AM
2	GMT + 5:30	Start Date 04/06/2010 05.30 AM	GMT + 5:30	04/06/2010 05.00	04/06/2010 05.00 AM

T
a
Table 2

2. If time zones of ITIM and Ace Server are different

   A. If ITIM time zone is GMT +/– **X: 00** and Ace Server time zone is GMT +/– **Y: 00**
   For example, ITIM time zone is GMT - 05:00 and Ace Server time zone is GMT + 06:00 you must set minutes as 0(refer case 1 from Table 3). If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer case 2 from Table 3).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5	Start Date 04/06/2010 06.00 PM	GMT + 6	04/07/2010 05.00	04/06/2010 06.00 PM
2	GMT -5	Start Date 04/06/2010 06.30 PM	GMT + 6	04/07/2010 05.00	04/06/2010 06.00 PM

Table 3

B. If ITIM time zone is GMT +/– **X: 30** and Ace Server time zone is GMT +/– **Y: 30.**
For example, ITIM time zone is GMT - 5:30 and Ace Server time zone is GMT + 6:30 you must set minutes as 0(refer case 1 from Table 4). If you do not set minutes as 0 then adapter will set it 0 on Ace Server (refer case 2 from Table 4).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:30	Start Date 04/06/2010 4.00AM	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.00 AM
2	GMT - 5:30	Start Date 04/06/2010 4.30AM	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.00 AM

Table 4

C. If ITIM time zone is GMT +/– **X: 00** and Ace Server time zone is GMT +/– **Y: 30.**
For example, ITIM time zone is GMT - 5:00 and Ace Server time zone is GMT + 6:30 you must set minutes as 30(refer case 1 from Table 5). If you do not set minutes as 30 then you will get minutes as 30 during reconciliation from Ace Server (refer case 2 from Table 5).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:00	Start Date 04/06/2010 05.30 AM	GMT + 6:30	04/06/2010 17.00	04/06/2010 05.30 AM
2	GMT - 5:00	Start Date 04/06/2010 05.00 AM	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.30 AM

Table 5

D. If ITIM time zone is GMT +/– **X: 30** and Ace Server time zone is GMT +/– **Y: 00.**
For example, ITIM time zone is GMT - 5:30 and Ace Server time zone is GMT + 6:00 you must set minutes as 30 (refer case 1 from Table 6). If you do not set minutes as 30 then you will get minutes as 30 during reconciliation from Ace Server (refer case 2 from Table 6).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:30	Start Date 04/06/2010 05.30 AM	GMT + 6:00	04/06/2010 17.00	04/06/2010 05.30 AM
2	GMT - 5:30	Start Date 04/06/2010 05.00 AM	GMT + 6:00	04/06/2010 16.00	04/06/2010 04.30 AM

Table 6

Supported Configurations

Installation Platform

The IBM Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:

Solaris 8
Solaris 9

Managed Resource:
RSA Authentication Manager (ACE/Server) v6.1 on Solaris

IBM Tivoli Identity Manager:
ITIM 4.6
ITIM Express 4.6

IMPORTANT NOTE:
This adapter manages ONLY version 6.1 of Authentication Manager (ACE).
This Adapter must be installed on the same server as the ACE system.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY  10504-1785
U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan
```

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

```
IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758 U.S.A.
```

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

End of Release Notes